Appendix E to DIR Contract No. DIR-SDD-1855

Sample Statement of Work

Customer name

Brad Miller
brad@solidborder.com

Scope of Work

Engagement Objectives

Customer, TX ("Customer or "Client") has requested PCI Data Security Standard ("DSS") compliance services focused on protecting sensitive credit card data that is stored, processed, and transmitted within the business environment. These services will also include a high-level PCI DSS gap analysis report outlining the control status (in place, not in place) for key PCI DSS control areas, including:

- High-level policies and procedures
- CDE network architecture
- Cardholder data encryption and key management
- CDE logging
- CDE penetration testing and vulnerability assessment

Scoping Considerations

Specific details relating to our understanding of the scope are listed below. This information has been provided by Customer through documents and/or interviews, and some assumptions may have been made based upon PCI DSS practices.

Significant variance from this information may incur additional labor or license fees and result in a Change Order. Should the noted scoping details be found inaccurate, the proposal will be revised to incorporate required changes.

Overview of Business Organization	• Merchant - Level 2-4 • Annual Compliance Deadline: 01/01/2012
Assessment Type	• PCI Pre-Assessment and DSS gap analysis
Cardholder Data Environment Systems components and locations that access, store, process or transmit cardholder data	• Up to one [**1**] applications for testing • Four [**4**] business units / departments with access to cardholder data • Physical Locations for testing ○ Up to three [**3**] of **40** Brick and Mortar Locations • System Components ○ Network Components for testing ▪ Up to two [**2**] of two [**2**] Perimeter Firewalls ▪ Up to four [**4**] of [**40**] Switches • Up to [**20**] interviews
Key Compliance Factors	• Centralized policies and procedures **are in place**. • Internal network segmentation (via firewalls or router / switch based ACLs) is **not in place**. Cardholder data **is not stored in clear text**. Formal key management processes **are not in place**. Logging **is enabled** for all system components. Logs **are** stored in a centralized log management system. Quarterly perimeter scans (via an ASV) a**re** taking place. • Annual perimeter and internal (application and network based) penetration tests **are not** taking place.

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security

Detailed Tasks and Approach

Fishnet Security employs a multi-phase methodology that is intended to identify all applications and system components that make up the cardholder data environment and review applicable policies and procedures as well as people, process and technology based controls against the PCI DSS. The following outlines our comprehensive approach to PCI compliance.

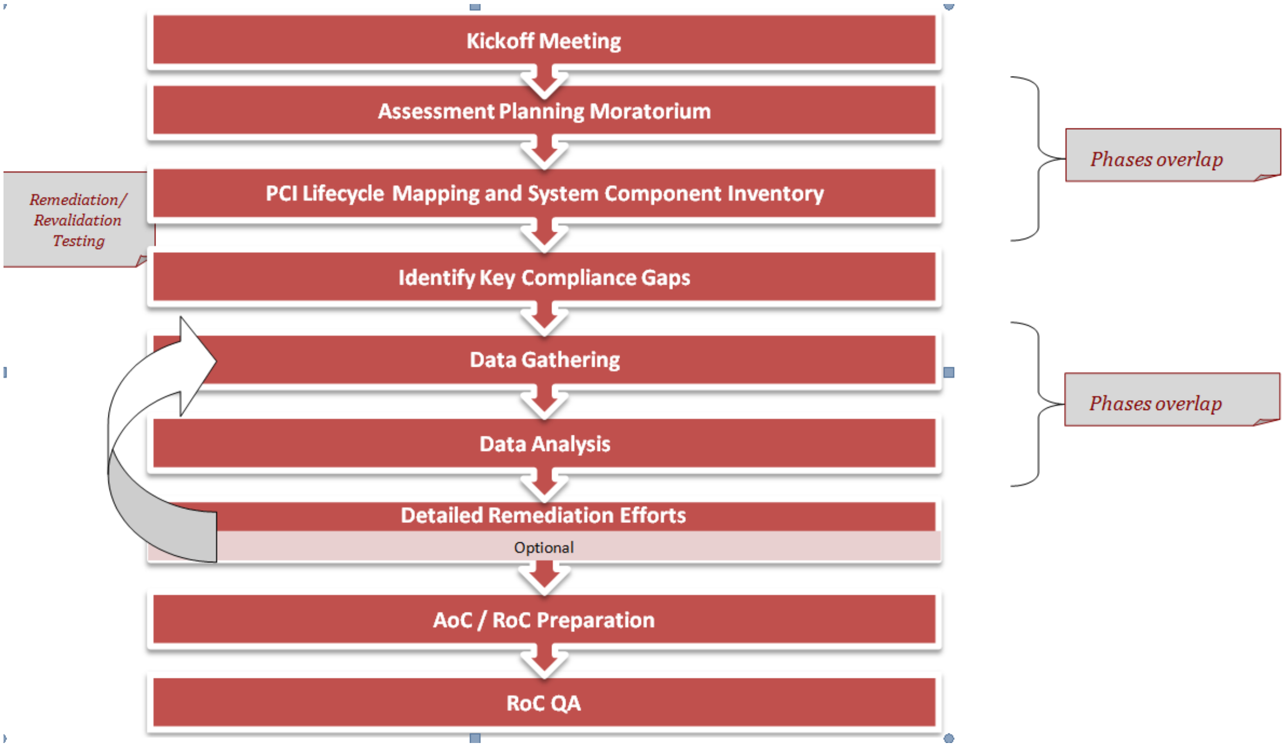
Pre-Assessment Overview

Fishnet Responsibilities

The intent of a PCI DSS assessment is to review the current compliance status (in place or not in place) of Customer's cardholder data environment ("CDE") as defined by the Client and the Qualified Security Assessor ("QSA"). The QSA's responsibilities are to review Customer's current compliance status; including:

- Policy and procedure review
- Network architecture review
- Application, system component and physical security configuration and controls review

The QSA's focus will be reviewing Customer's current compliance status. If the QSA is inquired to comment on or be involved in activities such as detailed remediation guidance or revalidation testing, the guidance provided will be "reasonable" within the context of the project delivery timeframe and Reoccurring remediation meetings and extensive written remediation expectations are not part of the scope, and will not be required from Fishnet Security.


Kickoff Meeting
Assessment Planning Moratorium
PCI Lifecycle Mapping and System Component Inventory
Identify Key Compliance Gaps
Data Gathering
Data Analysis
Detailed Remediation Efforts
Optional
AoC / RoC Preparation
RoC QA
Remediation/ Revalidation Testing
Phases overlap
Phases overlap

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security

Appendix E to DIR Contract No. DIR-SDD-1855

Sample Statement of Work: Customer

Assessment Preparation and Kickoff

Kickoff Meeting

- Discuss anticipated dates for on-site work
- Confirm PCI certification deadline
- Review and distribute initial data gathering requests

Assessment Planning

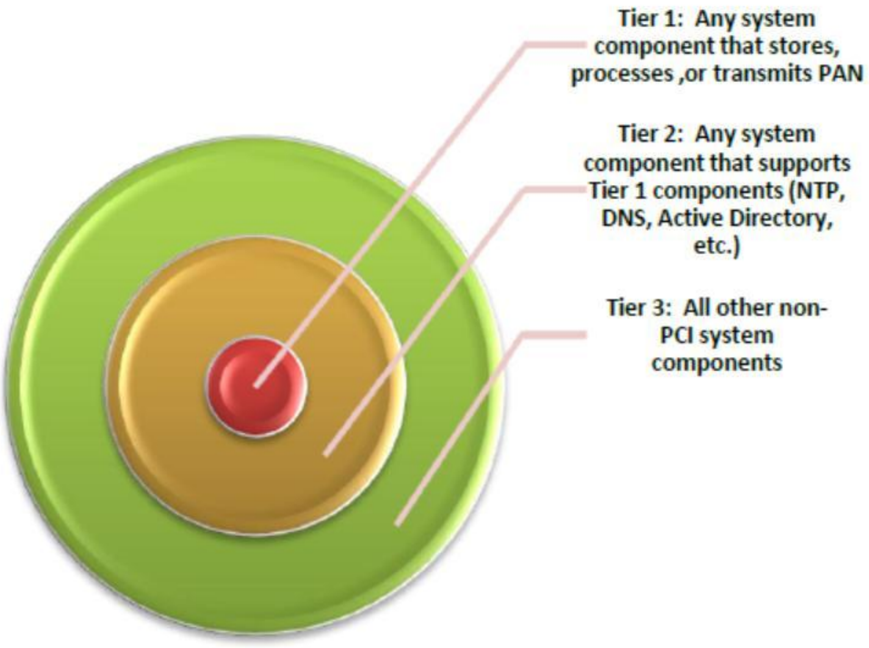
- Client will gather all initial data requests and distribute them to Fishnet Security
- Client will work with Fishnet Security to identify various subject matter experts and formally schedule interviews during the initial on-site visit (or remotely via conference call); Client will provide Fishnet Security with a formal interview schedule prior to any on-site work.
- Fishnet Security will conduct initial scoping and discovery meetings via conference call (optional).

NOTE: Prior to commencing any on-site work, we require a two-week (10 business days) assessment planning moratorium to ensure that initial documentation requests are gathered and provided and that a formal interview schedule is developed and agreed upon. Without this necessary planning time, we will be unable to ensure various assessment efficiencies. If on-site work is required inside of this moratorium period, project delays or overages could occur and a Change Order may be required.

PCI Lifecycle Mapping and System Component Inventory

- Fishnet Security will inventory and confirm all in-scope applications and related system components.
- Fishnet Security will identify and confirm all PCI dataflows and lifecycles that store, process or transmit cardholder data.
- Fishnet Security will classify all applications and systems components as Tier 1, Tier 2, and or Tier 3.
- Fishnet Security will identify samples to be used during the assessment process.

PCI System Component Tier Classifications


Tier 1: Any system component that stores, processes ,or transmits PAN
Tier 2: Any system component that supports Tier 1 components (NTP, DNS, Active Directory, etc.)
Tier 3: All other non-PCI system components

Sample Statement of Work: Customer Name

Identify Key Compliance Gaps

- Validate that centralized policies and procedures are in place
- Validate internal network segmentation (via firewalls or router/switch based ACLs) is in place
- Validate that cardholder data is not stored in clear text
- Validate that formal key management processes are in place
- Validate that logging is enabled
- Validate that logs are stored in a centralized log management system
- Validate quarterly perimeter (via an ASV) and internal vulnerability scans are taking place
- Validate annual perimeter and internal (application- and network-based) penetration testing is taking place

PCI On-Site Review

Data Gathering

- Conduct technical interviews with business process owners, application and system component administrators, and other supporting personnel.
- Client personnel will facilitate all data gathering efforts.
- Fishnet Security will support data gathering efforts by providing specific data requests to necessary personnel.

Data Analysis

- Review policies, procedures, and processes utilized to protect the cardholder data environment
- Conduct technical analysis of controls infrastructure covering Tier 1 and Tier 2 PCI applications and system components
- Create a gap analysis matrix that identifies all non-compliant PCI DSS controls
- Provide high-level remediation guidance non-compliant controls

Detailed Remediation Efforts (Optional)

- Fishnet Security can help Client remediate any control gaps that are identified during the Data Analysis phase.
- Any detailed remediation assistance will be subject to a Change Order or a new Statement of Work

What happens if Customer enters a state of revalidation?

To help ensure the timeliness of information that is provided to the card brands and/or merchant acquirers, the PCI Security Standards Council ("SSC") has instituted a requirement for revalidation testing for any assessments that enter a prolonged state of compliance validation. Fishnet Security formally defines this prolonged state as 120 days starting on the first day of on-site work. If the Data Analysis phase is not completed within 120 days, Customer will be subject to revalidation testing.

If Fishnet Security enters into a state of revalidation, Fishnet Security will have to revalidate that a specific subset of controls are still in a compliant state. All controls that are subject to revalidation testing will have to be retested to ensure their state of compliance. The subset of controls includes:

- Section 1
- Section 3

Section 6

Section 7

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security

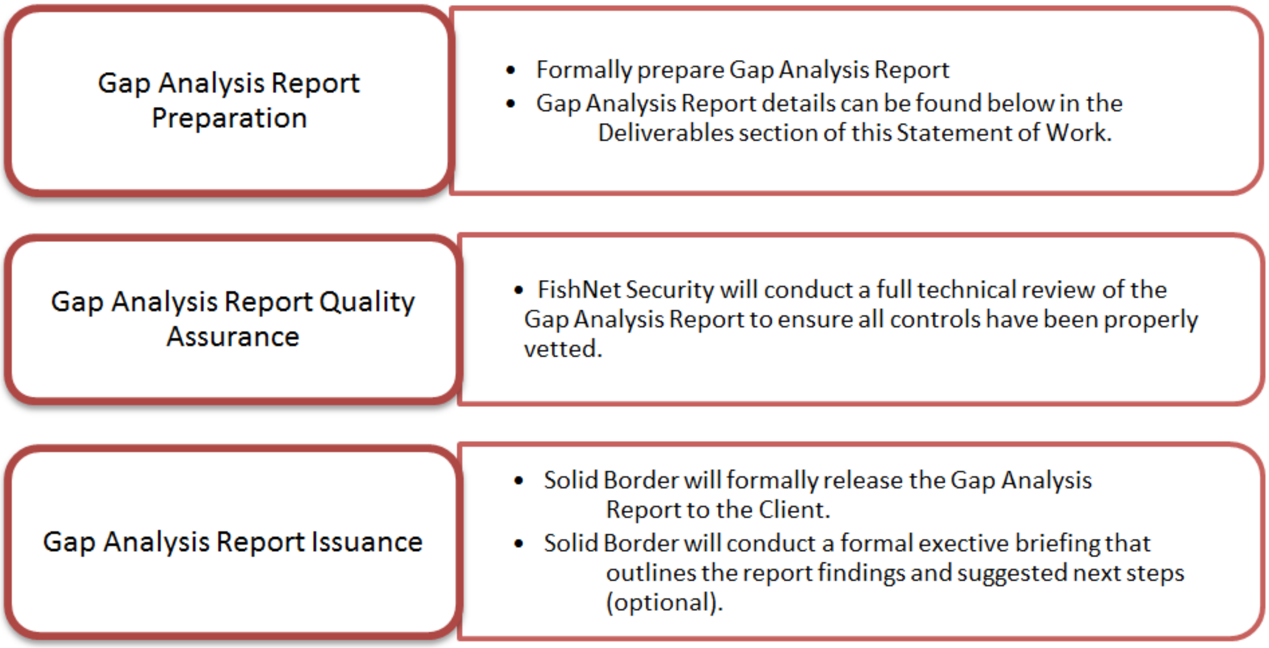
If the Data Analysis phase has not completed within 270 days of the initial on-site visit, revalidation testing will have to be performed on all controls.

Some of the common reasons that companies enter a state of revalidation include:

- The client enters a state of remediation and cannot complete all remediation activities (including retesting by Fishnet Security) in a timely manner.
- The client is unorganized or is unable to provide Fishnet Security with the proper data required to demonstrate compliance in a timely manner.
- The client incorporates major changes to its cardholder data environment during the assessment, thus requiring Fishnet Security to review the incorporated changes.

As Fishnet Security cannot fully anticipate the level of effort required for revalidation testing at the onset of the assessment, a formal Change Order will be prepared by Fishnet Security that will appropriately cover all revalidation testing required to successfully complete the assessment.

Gap Analysis Reporting



Gap Analysis Report Preparation

- Formally prepare Gap Analysis Report
- Gap Analysis Report details can be found below in the Deliverables section of this Statement of Work.

Gap Analysis Report Quality Assurance

- FishNet Security will conduct a full technical review of the Gap Analysis Report to ensure all controls have been properly vetted.

Gap Analysis Report Issuance

- Solid Border will formally release the Gap Analysis Report to the Client.
- Solid Border will conduct a formal exective briefing that outlines the report findings and suggested next steps (optional).

Deliverables

Pre-Assessment Report

The Pre-Assessment Report will outline the current scope of the cardholder data environment and the compliance status for key control areas. The Pre-Assessment Report will include:

- Executive Summary – This section of the report will provide Customer with an executive overview of the cardholder data environment and a high-level prioritized remediation roadmap.

- PCI Environment Discovery and Scoping – This section of the report will provide Customer with an overview of its cardholder data environment, including:
    - Tier 1 Applications and System Components – Applications and systems that directly store, process, or transmit cardholder data or are located on the same network as said applications and systems
    - Tier 2 System Components – System components that support the Tier 1 environment (i.e., Active Directory, NTP, DNS, Anti-virus, patching servers, etc.)
    - Tier 3 System Components – All other non Tier 1 and Tier 2 system components
- Compliance Status Overview – This section of the report will outline any identified compliance gaps and suggested remediation steps for key control areas, including:
    - Policy compliance
    - Data encryption and key management practices
    - Application and system component logging
    - Network segmentation
    - Vulnerability scanning and penetration testing

Dependencies and Assumptions

The following terms are set forth to determine the roles and responsibilities that both parties are to maintain. This is done to eliminate confusion and prevent delays in on-site data gathering. Failure to maintain these terms may result in extended on-site data collection, additional labor fees, and related travel expenses to cover the extra time spent on-site.

- Fishnet Security will not begin to provide the Services as described until Customer has returned the signed SoW.
- Scope based on PCI DSS at time of SoW creation. Unforeseen changes to the PCI DSS that may impact the scope of the project will be addressed by a mutually agreed upon Change Order as needed.
- In order to ensure the accurate and timely success of the engagement, Customer must provide Fishnet Security with the following Conditions:
    - Seventy-two (72) hours prior to the start of the PCI Assessment, Customer's IT security policies, standards and procedures, any PCI equipment inventory, credit card data flow map(s), and network infrastructure map(s);
    - Complete PCI device inventory
    - Credit card data flow maps
    - Network infrastructure maps
    - All Documentation relating to the existing network configuration, servers, applications, databases and other supporting system components
    - A formal interview scheduled outlining topics, meeting times and expected attendees
- This SoW shall terminate twelve (12) months from the SoW Effective Date or upon the completion of the Services. Fishnet Security will contact Customer within five (5) business days from the SoW Effective Date to initiate the PCI Assessment. Upon contact, Customer and Fishnet Security will mutually determine a date to begin the on-site portion of the PCI Assessment. If Customer provides all Conditions as stated in above, Fishnet Security will provide the ROC within six (6) weeks of the date Fishnet Security initiates the on-site portion of the PCI Assessment.
- If Customer does not fully comply with the PCI DSS requirements within 120 days from the first day of onsite work, Fishnet Security will not attest to Customer's PCI DSS compliance and will not provide the ROC until a period of revalidation testing is complete. Revalidation testing estimates and costs have not been included in this statement of work and are subject to a change

request. Per Fishnet Security's revalidation testing definition, sections 1, 3, 6, 7 and 11 of the PCI DSS will require full retesting. If Customer does not fully comply with the PCI DSS within 270 days of the initial onsite visit, revalidation testing will have to be completed on all PCI DSS controls. Fishnet Security requires the foregoing timeframes so that any changes or updates in Customer's IT security environment that may have occurred since the original PCI Assessment will be identified and taken into consideration concerning Customers compliance to the PCI DSS Standard.

- Scoped pricing for PCI On-Site Engagements is based upon the information provided by Customer via initial discovery documents and conversations with Fishnet Security prior to the start of the engagement. Fishnet Security assumes the client has centralized policies, centralized system management, internal network segmentation (i.e., devices used to limit network traffic that can access PCI impacted systems and data), and external perimeter segmentation (firewalls) in place.
- Additional Cardholder Data ("CHD") applications found during discovery phase of the engagement, not stated in scope of work, will incur additional scoping, services or fees.
- Fishnet Security assumes that all Customer data gathering activities will be executed in an efficient manner and data promptly submitted to Fishnet Security consultants. Any delays incurred in acquiring this information may result in the need for a mutually agreed upon Change Order.
- Fishnet Security will not perform any additional work outside of the services described in this SoW without the expressed permission of authorized Customer personnel; including a signed Change Order.

Appendix E to DIR Contract No. DIR-SDD-1855

Sample Statement of Work: Customer Name

- Customer will designate one employee to serve as a primary Point of Contact ("POC") for the Fishnet Security project team. The designated POC will be responsible for, and have authority to schedule Client resources for required meetings, interviews, and other needs deemed necessary to complete the project work within the specified project parameters, as well as to be responsible for all final decisions with respect to this Scope of Work. Customer POC will participate in weekly status meetings and serve as the first point of escalation for any project related requests or issues.
- Customer is responsible for notifying impacted personnel of the testing as needed, and said testing is conducted with the expressed authority of management.
- Customer will provide access to all proprietary information, applications, and systems necessary to the success of this project.
- For multi-year contracts, Fishnet Security will need to revisit contract total each year and considers inflation, adjustments to PCI DSS standard, and any changes in the Customer environment prior to engagement. A Change Order will be requested for any additional fees and/or adjustments in the pricing.
- No Fishnet Security employee is expected to work more than ten (10) consecutive hours.
- Any special conditions, not stipulated at the time of this quotation, such as late evening/early morning hour requirements (Monday-Friday 5PM-8AM and weekends), may result in additional fees and may require a Change Order.
- Travel: Travel expenses shall be reimbursed in accordance with Section 4.G of DIR Contract No. DIR-SDD-1855.
- If Customer cancels or reschedules Services within five (5) days of the scheduled start date, Customer shall reimburse Fishnet Security for two (2) days of Services as defined in the SOW (rate multiplied by number of resources) or $3,500, whichever is less. Non-refundable and nontransferable travel expenses will be billed by Fishnet Security to Customer at actual cost.

Project Management

Project Management Overview

As an initiative-focused engagement, maintaining clear channels of communication will be necessary to ensure success. Fishnet Security will conduct status meetings, including documented briefings on project status, issues noted, and issues addressed as they relate to schedule, deliverables, project quality, and team interaction. In addition to these scheduled briefings, Solid Border will provide immediate notification of issues requiring Customer action or intervention. Fishnet Security expects the prompt resolution of any issues identified by our team members, as well as by Customer, to have minimal impact on the project timelines.

Responsibilities

The following list details Fishnet Security’s project management responsibilities for this engagement:

- Facilitation of the engagement kick-off meeting
- Management of project budget and Change Order process (if needed)
- Coordination of Fishnet Security personnel logistics
- Status report preparation and delivery on regular intervals as determined by Customer ’s engagement leader
- Ensure deliverables meet the Customer sponsor’s approval within the boundaries of the scope of the engagement
- Ensure engagement work is completed as agreed upon in this SoW and obtain Customer sign-off

Additional project management services beyond the responsibilities listed above can be provided at an additional cost and will be agreed upon prior to signature of this SoW.

Project Plan and Estimated Timelines

Detailed timelines and milestones will be further discussed and developed upon choosing Fishnet Security as the selected security services provider. Our consultants can typically be available within two to four weeks of signature of this SoW. Fishnet Security is committed to completing the project within a timeframe that is agreed upon with Customer.

Estimated Project Schedule	
Tasks	Estimated Duration*
Pre-Assessment and Gap Analysis	20 - 25 days

*Please note – time estimates include all labor and documentation. The above timeline is an estimate used for example purposes. The specific schedule will be determined collaboratively between Solid Border and Customer at engagement commencement and may vary based on client availability and environment.

Project Change Control

In the process of an engagement, additional work may be required based upon on-site discovery or changes requested by Customer. If variations from the original SoW are deemed necessary, a mutually agreed-upon Change Order will be created. Fishnet Security will provide a Change Order for Customer to review and sign before any work outside the original scope is performed or additional expenses are invoiced to Customer.

The Change Order will specifically address the work, software, or other items added to the SoW and the associated costs. A brief explanation of the requirements for the changes will also be included.

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security

Security and Privacy

Ensuring the security and privacy of your information is paramount. Our employees are guided by strict information security handling procedures to maintain a high level of security.

- All employees are subjected to criminal history background investigation as a condition of hire.
- All employees have agreed to and signed non-disclosure agreements.
- Data files maintained on portable computers (laptops) will be encrypted.
- Communications of sensitive “Client Confidential” data will be encrypted.
- Physical (paper) files and reports will be secured in locked offices and/or file cabinets.
- Client data files are destroyed after one year unless agreed to differently via client contract or industry/regulatory requirement.

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security

Appendix E to DIR Contract No. DIR-SDD-1855

Statement of Work: SB4021Customer

Pricing – please reference Solid Border Quote for pricing.

Signature Page

This work order is between Solid Border, Inc. (work to be done by Fishnet Security) and Customer is subject to the provisions of DIR Contract No. DIR-SDD-1855 The following signature authorizes the execution of the above statement of work. If this statement of work is acceptable, please sign, date and fax to 800.887.9974.

Customer Signature:

____
Signature

____
Printed Name

____
Date

Solid Border, Inc. Signature:

____
Signature

____
Printed Name

____
Date

Appendix E to DIR Contract No. DIR-SDD-1855

Fishnet Security